Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended)
Claim 2 (cancelled)
Claim 3 (currently amended)
Claim 4 (previously amended)
Claim 5 (cancelled)
Claim 6 (previously amended)
Claim 7 (previously amended)
Claim 8 (previously amended)
Claim 9 (original)
Claim 10 (currently amended)
Claim 11 (previously amended)
Claim 12 (previously amended)
Claim 13 (cancelled)
Claim 14 (currently amended)
Claim 15 (cancelled)
Claim 16 (cancelled)
Claim 17 (currently amended)
Claim 18 (cancelled)
Claim 19 (cancelled)

Claim 20 (cancelled)

Claim 21 (cancelled)

Claim 22 (new)

Claim 23 (new)

1. (Currently Amended)

A system for maintaining electronic data files and manifests for such data files stored in a third party data repository system, comprising:

a communications environment having:

(i) a first agent program for a depositor computer of an electronic data file in the data repository system which first agent program is a secure extension of the depositor computer;

(ii) a second agent program for a first user computer with access privileges to the electronic data file which second agent program is a secure extension of the first user computer;

(iii) electronic data files are encrypted so that an administrator of the repository system does not have access to said electronic data file in the clear;

a manifest for the electronic data file listing access controls for the electronic data file, the manifest being accessible to and maintained by the first agent program;

a first record of the first user computer's access privileges to the electronic data file, the first record being accessible to and maintained by the second agent program;

means to communicate changes to the manifest affecting the first user computer's access privileges to the electronic data file from the first agent program to the second agent program for updating the first record; and

means for the first agent program to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program whereby access by the repository administrator to the electronic data file and records of the user access privileges are restricted .

2. (Cancelled)

3. (Currently Amended)

The secure system, according to claim [[13]] 1, further comprising means for communicating the changes to the manifest affecting the first user computer's access privileges to the electronic data file from the second agent program to the first user computer.

4. (Previously Amended)

The secure system, according to claim 3, further comprising:

a third agent program for a second user computer with access privileges to the electronic data file which third agent program is a secure extension of the second user computer;

a second record of the second user computer's access privileges to the electronic data file, the record being accessible to and maintained by the third agent program,

wherein the means to communicate changes to the manifest affecting the first user computer's access privileges to the electronic data file from the first agent program to the second agent program for updating the first record, comprises means to communicate changes to the manifest affecting the second user computer's access privileges to the electronic data file from the first agent program to the third agent program for updating the second record; and

wherein the means for the first agent program to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program, comprises means for the first agent program to verify the second user computer's access privileges to the electronic data file before the electronic data file is released to the third agent program.

5. (Cancelled)

6. (Previously Amended)

The secure system, according to claim 4, further comprising means for communicating the changes to the manifest affecting the second user computer's access privileges to the electronic data file from the third agent program to the second user computer.

7. (Previously amended)

The secure system, according to claim 4, wherein the communication environment comprises a server.

8. (Previously amended)

The secure system, according to claim 4, further comprising an interface to the data repository system housed in the communications environment, the interface adapted to receive all communications to and from the data repository system and the agent programs.

9. (Original)

The secure system, according to claim 8, wherein the interface is a secure extension of the data repository system.

10. (Currently Amended)

A process for maintaining a secure electronic data search system for a third party electronic data repository which contains document data files encrypted to make them secure from the administrator of the repository, the system having a manifest listing access controls for each electronic data file stored in the data repository and a record maintained by a documents originator listing document access privileges for each computer with access to the electronic data stored in the repository which record is maintained secure from the administrator of the

repository, the process comprising the steps performed by the documents originator of:

updating a manifest for an electronic data file stored in the repository;

identifying all computers with a change in access to the electronic data file effected by the update;

updating the access privileges records of all affected computers; [[and]]

communicating the updated access privilege records to the affected computers; and

providing the originators of the electronic data files, users of the electronic data files and the repository administrator with vaults which are secure extensions of their respective work spaces.

11. (Previously Amended)

A secure system for searching electronic data files stored in a data repository system in which the documents are encrypted to make them secure from the repository administrator, comprising:

means for a data file originator maintaining a manifest listing access controls for each electronic data file stored in the data repository system secure from the repository administrator;

means for restricting access to each manifest to a computer with deposit privileges for the electronic data file;

means for maintaining a record listing access privileges of users of the data file to the electronic data files associated with each computer with access privileges to at least one electronic data file in the data repository system;

means in the computer with deposit privileges for restricting access to each said record to the associated computer with access privileges; and

means for updating the record associated with each computer affected by an access change in a manifest.

12. (Previously Amended)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for an electronic data repository which contains data files that are encrypted to maintain them secure from the repository administrator, the system having a manifest listing access controls for each electronic data file stored in the data repository and a record secure to the document originator listing document access privileges for each computer with access to electronic data stored in the repository, the program product performed by the data files originator comprising:

software for updating a manifest for an electronic data file stored in the repository;

software for identifying all computers with a change in access to the electronic data file effected by the update;

software for communicating the change in access to all affected computers;

software for updating the access privileges records of all affected computers; and

software for communicating the updated access privilege records to the affected computers.

13. (Cancelled)

14. (Currently Amended)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for a third party electronic data repository in which electronic data file documents are stored in encrypted form in the data repository to prevent access by the repository administrator such a system having a manifest to an electronic data document secure to the originator of the electronic document listing document access privileges for each computer with access to the electronic data document stored in the repository, the program product comprising:

software for updating the manifest for the electronic data file document stored in the repository;

software for identifying all computers with access to the electronic data file document and for changing such access in an update software for communicating the change in access to all affected computers;

software for updating access privileges records in all affected software; [[and]]

software for communicating the access privilege records to the affected computers; and

software for maintaining vaults for each of the originators of the electronic data files, users of the electronic data files and the repository administrator as secure extension of their respective work spaces.

15. (Canceled)

16. (Cancelled)

17. (Currently amended)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for a third party electronic data repository in which electronic data file documents are stored in encrypted form in the data repository to prevent access by the repository administrator such a system having a record listing document access privileges for each computer with access to electronic data stored in the repository the program product comprising:

software for updating a manifest for an electronic data file document stored in the repository;

software for identifying all computers with access to the electronic data file document and for changing such access in an update software for communicating the change in access to all affected computers;

software for updating access privileges records in all affected software; and

software for communicating the access privilege records to the affected computers;

software in [[the]] a vault of the document originator to encrypt a document that it receives from the originator, prior to forwarding it [[on to]] onto the electric data vault of the repository;

software in [[the]] a vault of the repository ~~administrator~~ which on receipt of the encrypted document, signs the encrypted document itself before storing the document in the electronic data repository and returns to the originator's vault proof of deposition of the encrypted document;

software in [[the]] a vault of a requesting user to request the repository's vault ~~to request~~ for use of the requested document;

software in he repository's vault to retrieve a copy of the document in encrypted form which is forwarded, along with the requester's identity, to the originator's vault;

software in the originator's vault to verify that the requester is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself;

software in the originator's vault when the requester has access to decrypt the document and forward the decrypted document directly to the requester's vault; and

software in the requester's vault to provide proof of receipt of the decrypted document wherein the originators of the electronic data files, users of the electronic data files and the repository administrator all have vaults which are secure extensions of their respective work space ~~wherein the originators of the electronic data files, users of the electronic data files and the repository administrator all have vaults which are secure extensions of their respective work space~~.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Cancelled)

22. (New)

A process for maintaining a secure electronic data search system for a third party electronic data repository which contains document data files encrypted to make them secure from the administrator of the repository, the system having a manifest listing access controls for each electronic data file stored in the data repository and a record maintained by a documents originator listing document access privileges for each computer with access to the electronic data stored in the repository which record is maintained secure from the administrator of the repository, the process comprising the steps performed by the documents originator of:

updating a manifest for an electronic data file stored in the repository;

identifying all computers with a change in access to the electronic data file effected by the update;

updating the access privileges records of all affected computers;

communicating the updated access privilege records to the affected computers;

providing the originators of the electronic data files, users of the electronic data files and the repository with vaults which are secure extensions of their respective work spaces;

encrypting in the vault of the document originator a document of the originator, prior to forwarding it on to the vault of the repository;

signing the encrypted document in the vault of the repository before storing the document in the electronic repository and returning to the originator's vault proof of deposition of the encrypted document;

sending from the vault of a requesting user to the repository's vault a request to use the requested document;

retrieving from the repository's vault a copy of the document in encrypted form and forwarding it along with the requester's identity, to the originator's vault;

verifying in the originator's vault that the requester is authorized to view the document from the access control list in the originators vault identifying access privileges for the document;

decrypting the document in the originator's vault when the requester has access and forwarding the decrypted document directly to the requester's vault; and

having the requester's vault provide proof of receipt of the decrypted document.

23. (New)

A computer program product on a computer usable medium for maintaining a secure electronic data search system for a third party electronic data repository in which electronic data file documents are stored in encrypted form in the data repository to prevent access by the repository administrator such a system having a manifest to an electronic data document secure to the originator of the electronic document listing document access privileges for each computer with access to the electronic data document stored in the repository, the program product comprising:

software for updating the manifest for the electronic data file document stored in the repository;

software for identifying all computers with access to the electronic data file document and for changing such access in an update software for communicating the change in access to all affected computers;

software in the vault of the document originator to encrypt a document that it receives from the originator, prior to forwarding it on to the vault of the repository administrator;

software in the vault of the repository which on receipt of the encrypted document, signs the encrypted document before storing the document in the electronic repository and returning to the originator's vault proof of deposition of the encrypted document;

software in the vault of a requesting user to the repository's vault to request use of the requested document;

software in repository's vault to retrieve a copy of the document in encrypted form which is forwarded, along with the requester's identity, to the originator's vault;

software in the originator's vault to verify that the requester is authorized to view the document using an access control list identifying access ownership privileges for the document stored in the vault itself;

software in the originator's vault when the requester has access decrypts the document and forwards the decrypted document directly to the requester's vault; and

software in the requester's vault to provide proof of receipt of the decrypted document.